Systém na zpracování informací o útocích z veřejných zdrojů a z Turrisu

Robert Šefr • robert.sefr@nic.cz • 28.05.2015

CZ.NIC | SPRÁVCE DOMÉNY CZ

Bezpečnostní incidenty v ČR?

- Dochází k nim?
  - Ano, otázkou je, jak je co nejdříve odhalit a eliminovat příčiny

- **Reaktivní přístup**
  - Zpracovávat hlášení incidentu od dalších CSIRTů
- **Proaktivní přístup**
  - Aktivně incidenty vyhledávat a začít řešit

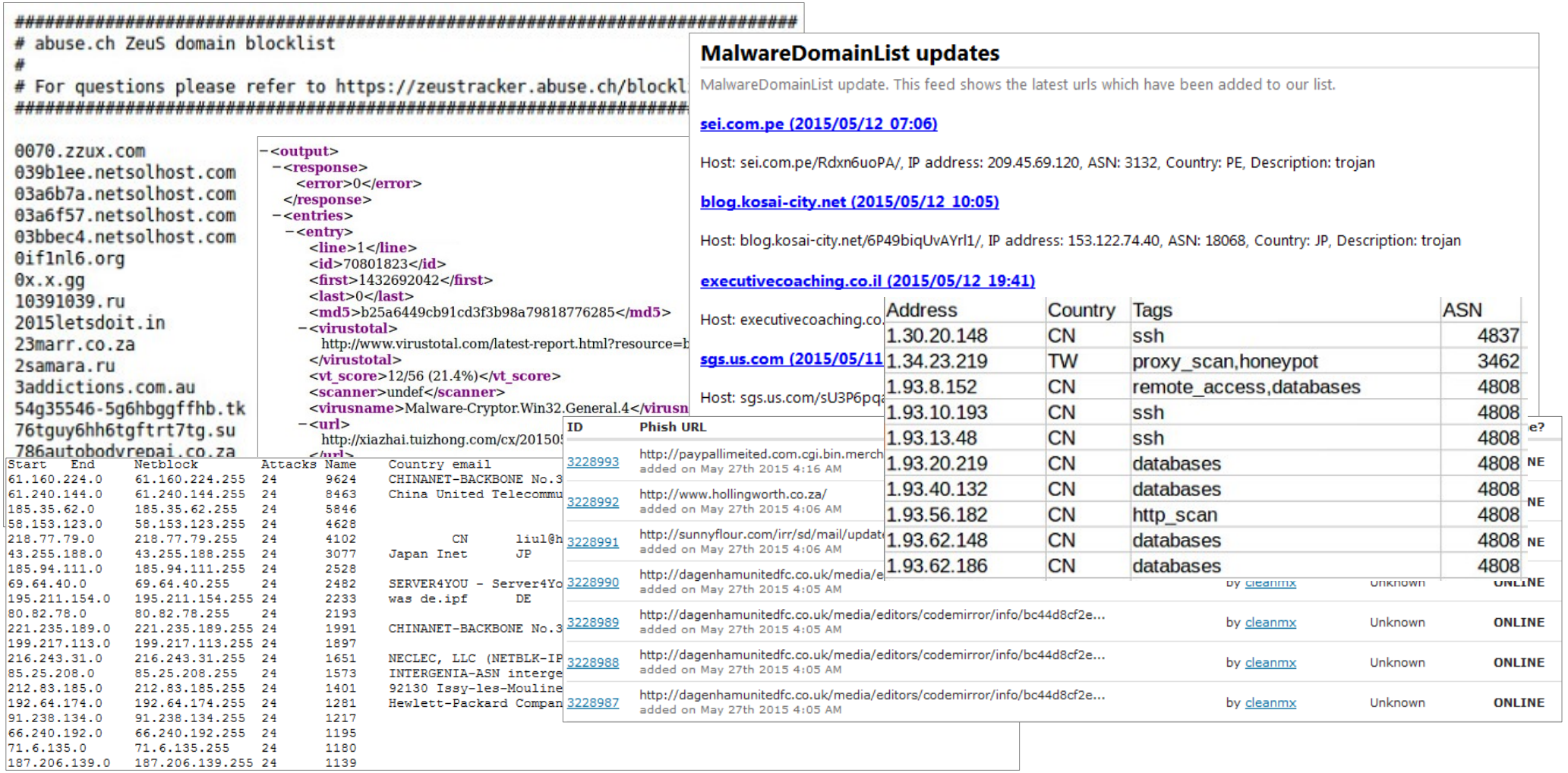
Zdroje informací o hrozbách

- Existuje mnoho projektů, které ukazují na problémové IP a domény
  - Shadowserver
  - Abuse.ch
  - Clean MX
  - Phishtank
  - Malwaredomainlist
  - **Turris Greylist** - https://www.turris.cz/cs/greylist
  - A mnoho dalších ...

Zdroj: zeustracker.abuse.ch (květen, 2015)

Mnoho různých formátů

Formáty: csv, xml, json, stix, openioc; **Metody doručení**: http, email, api



```
################################################################################
# abuse.ch ZeuS domain blocklist
#
# For questions please refer to https://zeustracker.abuse.ch/blockl
################################################################################

0070.zzux.com
039b1ee.netsolhost.com
03a6b7a.netsolhost.com
03a6f57.netsolhost.com
03bbec4.netsolhost.com
0if1nl6.org
0x.x.gg
10391039.ru
2015letsdoit.in
23marr.co.za
2samara.ru
3addictions.com.au
54g35546-5g6hbggffhb.tk
76tguy6hh6tgftrt7tg.su
786autobodyrepai.co.za
```

```
−<output>
 −<response>
    <error>0</error>
  </response>
 −<entries>
  −<entry>
    <line>1</line>
    <id>70801823</id>
    <first>1432692042</first>
    <last>0</last>
    <md5>b25a6449cb91cd3f3b98a79818776285</md5>
   −<virustotal>
      http://www.virustotal.com/latest-report.html?resource=b
    </virustotal>
    <vt_score>12/56 (21.4%)</vt_score>
    <scanner>undef</scanner>
    <virusname>Malware-Cryptor.Win32.General.4</virusn
   −<url>
      http://xiazhai.tuizhong.com/cx/20150
    </url>
```

MalwareDomainList updates

MalwareDomainList update. This feed shows the latest urls which have been added to our list.

sei.com.pe (2015/05/12_07:06)

Host: sei.com.pe/Rdxn6uoPA/, IP address: 209.45.69.120, ASN: 3132, Country: PE, Description: trojan

blog.kosai-city.net (2015/05/12_10:05)

Host: blog.kosai-city.net/6P49biqUvAYrl1/, IP address: 153.122.74.40, ASN: 18068, Country: JP, Description: trojan

executivecoaching.co.il (2015/05/12_19:41)

Host: executivecoaching.co.

sgs.us.com (2015/05/11

Host: sgs.us.com/sU3P6pq

Address	Country	Tags	ASN
1.30.20.148	CN	ssh	4837
1.34.23.219	TW	proxy_scan,honeypot	3462
1.93.8.152	CN	remote_access,databases	4808
1.93.10.193	CN	ssh	4808
1.93.13.48	CN	ssh	4808
1.93.20.219	CN	databases	4808
1.93.40.132	CN	databases	4808
1.93.56.182	CN	http_scan	4808
1.93.62.148	CN	databases	4808
1.93.62.186	CN	databases	4808

Start	End	Netblock	Attacks	Name	Country email
61.160.224.0	61.160.224.255	61.160.224.255	24	9624	CHINANET-BACKBONE No.3
61.240.144.0	61.240.144.255	61.240.144.255	24	8463	China United Telecommu
185.35.62.0	185.35.62.255	185.35.62.255	24	5846	
58.153.123.0	58.153.123.255	58.153.123.255	24	4628	
218.77.79.0	218.77.79.255	218.77.79.255	24	4102	CN liul@h
43.255.188.0	43.255.188.255	43.255.188.255	24	3077	Japan Inet JP
185.94.111.0	185.94.111.255	185.94.111.255	24	2528	
69.64.40.0	69.64.40.255	69.64.40.255	24	2482	SERVER4YOU - Server4Yo
195.211.154.0	195.211.154.255	195.211.154.255	24	2233	was de.ipf DE
80.82.78.0	80.82.78.255	80.82.78.255	24	2193	
221.235.189.0	221.235.189.255	221.235.189.255	24	1991	CHINANET-BACKBONE No.3
199.217.113.0	199.217.113.255	199.217.113.255	24	1897	
216.243.31.0	216.243.31.255	216.243.31.255	24	1651	NECLEC, LLC (NETBLK-IP
85.25.208.0	85.25.208.255	85.25.208.255	24	1573	INTERGENIA-ASN interge
212.83.185.0	212.83.185.255	212.83.185.255	24	1401	92130 Issy-les-Mouline
192.64.174.0	192.64.174.255	192.64.174.255	24	1281	Hewlett-Packard Compan
91.238.134.0	91.238.134.255	91.238.134.255	24	1217	
66.240.192.0	66.240.192.255	66.240.192.255	24	1195	
71.6.135.0	71.6.135.255	71.6.135.255	24	1180	
187.206.139.0	187.206.139.255	187.206.139.255	24	1139	

ID	Phish URL			
3228993	http://paypallimeited.com.cgi.bin.merch added on May 27th 2015 4:16 AM			
3228992	http://www.hollingworth.co.za/ added on May 27th 2015 4:06 AM			
3228991	http://sunnyflour.com/irr/sd/mail/updat added on May 27th 2015 4:06 AM			
3228990	http://dagenhamunitedfc.co.uk/media/e added on May 27th 2015 4:05 AM	by cleanmx	Unknown	ONLINE
3228989	http://dagenhamunitedfc.co.uk/media/editors/codemirror/info/bc44d8cf2e... added on May 27th 2015 4:05 AM	by cleanmx	Unknown	ONLINE
3228988	http://dagenhamunitedfc.co.uk/media/editors/codemirror/info/bc44d8cf2e... added on May 27th 2015 4:05 AM	by cleanmx	Unknown	ONLINE
3228987	http://dagenhamunitedfc.co.uk/media/editors/codemirror/info/bc44d8cf2e... added on May 27th 2015 4:05 AM	by cleanmx	Unknown	ONLINE

Mnoho typů informací

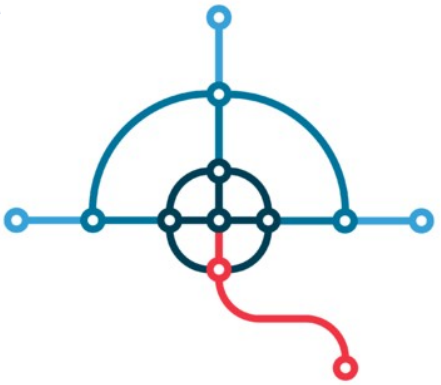
- Domény a URL hostující malware
- IP adresy aktivně napadající cizí stroje
- IP adresy Command & Control center botnetu
- IP adresy stojů ovládané botnetem
- Phishing URL

Automatizované vyhodnocování zdrojových feedů

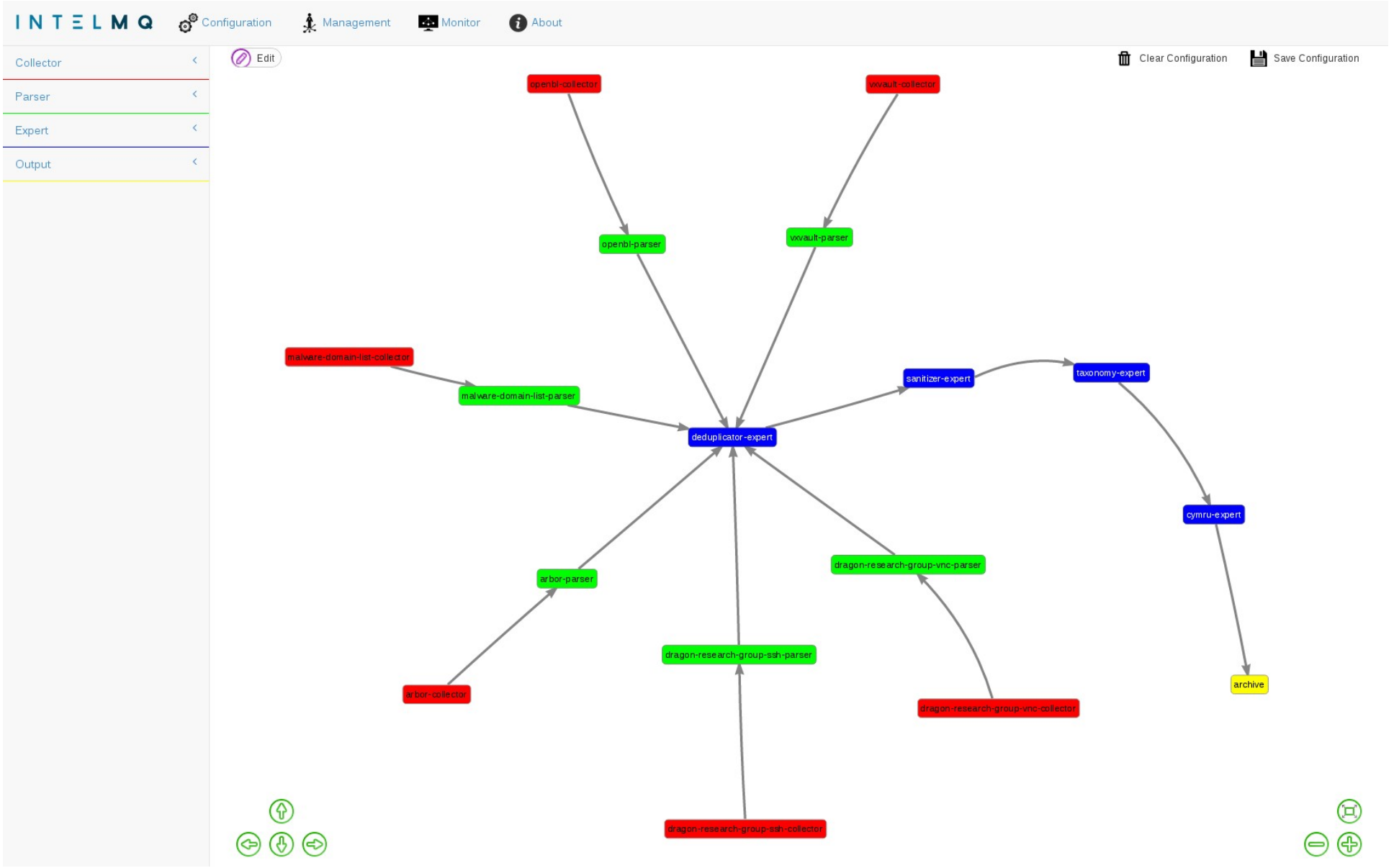
- Abusehelper
  - http://abusehelper.be/
- Megatron
  - https://github.com/cert-se/megatron-java
- Collective Intelligence Framework
  - http://csirtgadgets.org/collective-intelligence-framework/
- **IntelMQ**
  - https://github.com/certtools/intelmq

IntelMQ

- Společný projekt více evropských CERT týmů
- Transparentní architektura a možnost vlastních úprav ve všech fázích zpracování informací
- Důraz na jednoduché doprogramování vlastních modulů



Architektura IntelMQ



Výstup z IntelMQ – notifikace

- Automatizace notifikací subjektů s českou IP
- Čtení kontaktu z databáze RIPE
- Denní email se všemi notifikacemi pro daný kontakt

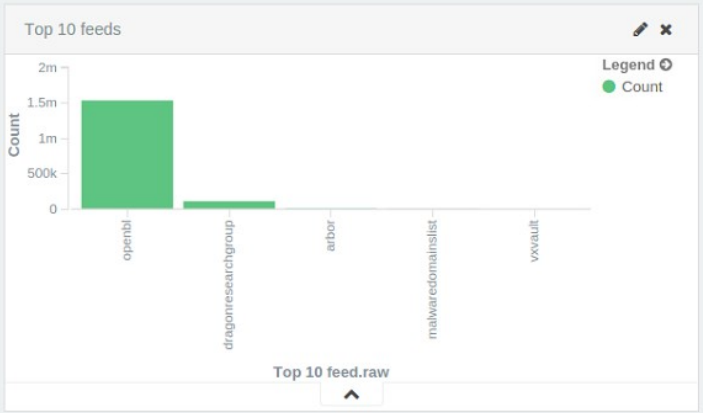
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Abuse contact for '192.168.100.0 - 192.168.100.255' is 'abuse@lir.net'

inetnum:        192.168.100.0 - 192.168.100.255
netname:        RIPE-NET1
descr:          /24 assigned
country:        NL
admin-c:        TP1-TEST
tech-c:         TP1-TEST
status:         ASSIGNED PA
mnt-by:         END-USER-MNT
changed:        dbtest@ripe.net 20020101
source:         TEST

% This query was served by the RIPE Database Query Service version 1.52.8 (UNDEFINED)
```

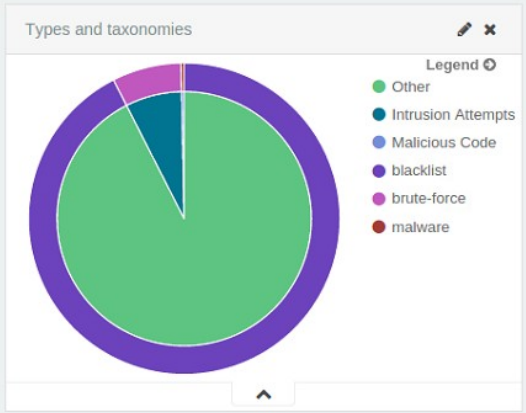
Výstup z IntelMQ – data pro Turris

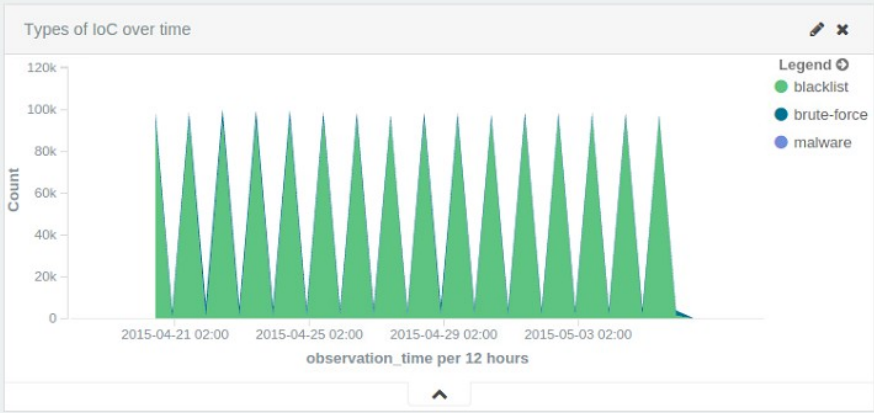
- Výstup z IntelMQ do databáze
- Podklady pro analýzu dat z Turrisu
  - Detekce infikovaných strojů za Turrisem
    - Aktivní vytváření spojení na malware IP
  - Upozornění na úspěšné útočníky
    - Úspěšně otevřená spojení a přenosy dat ze skenovacích a bruteforcing IP

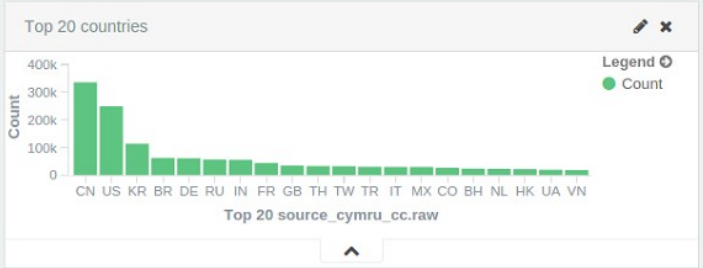
Výstup z IntelMQ – analýza a filtrace

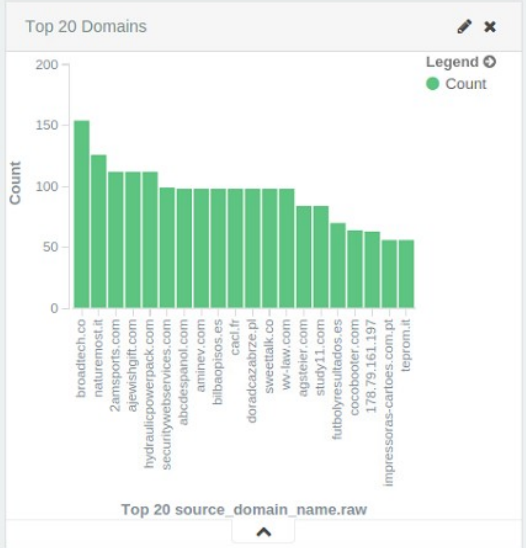
- Nástroje Elasticsearch, Logstash a Kibana

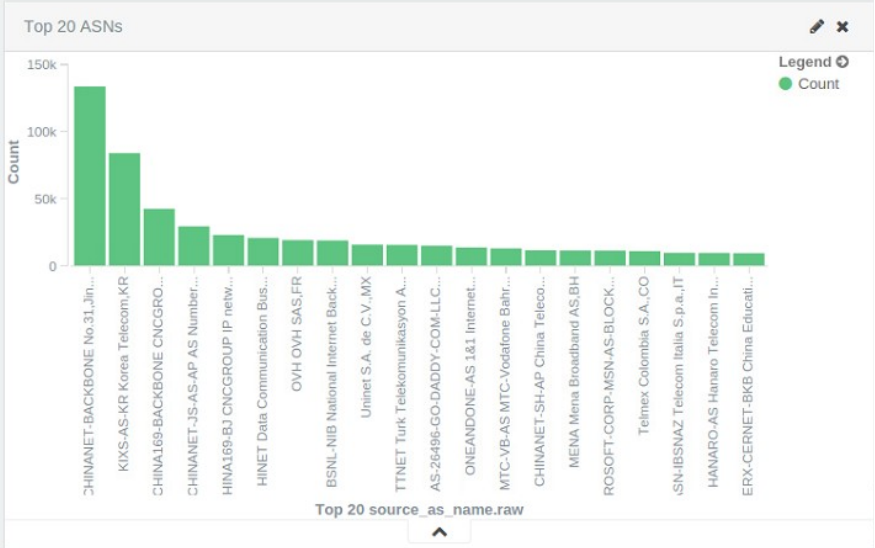












Další zdroje informací

- ENISA
  - https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information
- Processing Intelligence Feeds with Open Source Software
  - https://www.first.org/resources/papers/conference2014/first_2014_-_kaplan-_aaron_-_ifas-ihap_20140625.ppt

Děkuji za pozornost

Robert Šefr • robert.sefr@nic.cz • @CZ_NIC